МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Телекоммуникационное оборудование защищенных сетей

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (в сфере связи, информационных и коммуникационных технологий)

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Телекоммуникационное оборудование защищенных сетей» являются обучение принципам построения и эксплуатации различных телекоммуникационных сетей и систем за счет изучения современных телекоммуникационных технологий и технических средств. А также приобретение студентами необходимого объема знаний в области обеспечения безопасности телекоммуникационных сетей и систем, архитектуры беспроводных сетей, стандартов и механизмов защиты, используемых для защиты информации в телекоммуникационных сетях и системах.

Студенты должны научиться использовать сочетание различных технологий, протоколов и телекоммуникационного оборудования.

Основными задачами дисциплины являются:

- ознакомление основными видами телекоммуникационного оборудования;
- рассмотрение протоколов взаимодействия телекоммуникационного оборудования;
- изучение особенностей использования протокола OSPF;
- изучение особенностей использования протокола BGP;
- изучение основных принципов и подходов к защите информации в разнотипных телекоммуникационных сетях и системах.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ПК-1 - Способность анализировать и оценивать защищенность программно-аппаратных средств защиты информации;

ПК-7 - Способность выбирать и применять технические средства защиты информации, обеспечивать их функционирование, проводить восстановление и замену отказавших компонентов.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

-виды телекоммуникационных сетей связи;

-основные угрозы безопасности информации в телекоммуникационных сетях связи;

-методы и алгоритмы обеспечения безопасности информации в телекоммуникационных сетях связи;

-основные параметры каналов телекоммуникационных сетей связи;

- технические концепции построения различных телекоммуникационных сетей связи;

-способы организации каналов, доступов в телекоммуникационных сетях связи.

Уметь:

-рассчитывать и выбирать основные параметры аппаратуры телекоммуникационной связи, исходя из требований к качеству канала; эксплуатировать оборудование телекоммуникационных сетей;

-осуществлять выбор оборудования и программного обеспечения для построения защищенных телекоммуникационных сетей связи;

- интегрировать телекоммуникационные сети связи в сетевую инфраструктуру предприятия, учитывая все аспекты обеспечения ее безопасности;

-осуществлять мониторинг телекоммуникационных сетей.

Владеть:

-навыками расчета и выбора основных параметров аппаратуры телекоммуникационной связи, исходя из требований к качеству канала;

-навыками эксплуатации оборудования телекоммуникационных сетей;

- навыками выбора оборудования и программного обеспечения для построения защищенных телекоммуникационных сетей связи;

-навыками интеграции телекоммуникационных сетей связи в сетевую инфраструктуру предприятия, учитывая все аспекты обеспечения ее безопасности; принципами мониторинга телекоммуникационных сетей.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов

	Всего	Семестр №9
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 116 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Введение в телекоммуникационное оборудование защищенных сетей Содержание учебного материала: - Определение защищенной сети передачи данных (ЗСПД) - Классификация телекоммуникационного оборудования по назначению и уровням модели OSI - Основные требования к оборудованию защищенных сетей (надежность, отказоустойчивость, безопасность, управляемость) - Нормативно-правовая база РФ в области применения сертифицированного оборудования (ФСТЭК, ФСБ, Минобороны) - Жизненный цикл оборудования защищенных сетей: закупка, установка, настройка, эксплуатация, утилизация
2	Архитектура защищенных сетей и место оборудования в структуре Содержание учебного материала: - Топологии защищенных сетей (звезда, кольцо, ячеистая, иерархическая) - Уровни защищенной сети: периметр, сегментация, ядро, доступ - Демилитаризованная зона (DMZ): назначение и используемое оборудование - Распределение функций между сетевыми устройствами (маршрутизация, коммутация, межсетевое экранирование, обнаружение вторжений) - Принципы резервирования оборудования (активный-активный, активный-пассивный)

№ п/п	Тематика лекционных занятий / краткое содержание
3	Модели угроз и требования к телекоммуникационному оборудованию Содержание учебного материала: - Основные угрозы для телекоммуникационного оборудования (НСД, перехват трафика, подмена устройства, атаки на протоколы, отказ в обслуживании) - Модель нарушителя для защищенных сетей (внешний и внутренний) - Требования к оборудованию по классам защищенности (по приказам ФСТЭК России) - Критерии выбора оборудования для сетей с различным уровнем конфиденциальности - Документирование требований к оборудованию в техническом задании
4	Классификация и сертификация телекоммуникационного оборудования по требованиям безопасности Содержание учебного материала: - Классы защищенности оборудования (от пятого до первого) - Системы сертификации ФСТЭК России и ФСБ России - Этапы сертификации оборудования для защищенных сетей - Сертифицированное vs. несертифицированное оборудование: риски и ограничения - Реестр сертифицированного телекоммуникационного оборудования в РФ
5	Защищенные коммутаторы (L2/L3): архитектура и функции безопасности Содержание учебного материала: - Принципы работы коммутаторов в защищенных сетях - Функции безопасности коммутаторов: VLAN, ACL (Access Control Lists), 802.1X (Port-Based Authentication) - Защита от атак на канальном уровне (MAC-flooding, ARP-spoofing, STP-атаки) - Функции DHCP Snooping, Dynamic ARP Inspection (DAI), IP Source Guard - Настройка портов безопасности (Port Security, MAC-адресация, ограничение числа MAC)
6	Защищенные маршрутизаторы: протоколы динамической маршрутизации в защищенном исполнении Содержание учебного материала: - Назначение маршрутизаторов в защищенных сетях - Протоколы динамической маршрутизации (OSPF, BGP, RIP) и их уязвимости - Защита протоколов маршрутизации: аутентификация (MD5, SHA), фильтрация маршрутов - Виртуальные маршрутизаторы (VRF) для изоляции трафика в одном устройстве - Примеры защищенных маршрутизаторов (Cisco, Juniper, отечественные - Элтекс, БУЛАТ)
7	Межсетевые экраны (МЭ) нового поколения (NGFW) Содержание учебного материала: - Классификация межсетевых экранов (пакетные фильтры, stateful, NGFW) - Функции NGFW: инспектирование трафика на прикладном уровне (DPI), обнаружение вторжений (IDS/IPS), фильтрация приложений - Управление политиками безопасности на NGFW (правила allow/deny/nat) - Топологии включения МЭ (транспортный режим, мост, шлюз) - Примеры сертифицированных NGFW в РФ (UserGate, ViPNet Coordinator, Check Point)
8	Устройства VPN-шлюзов и криптомаршрутизаторы Содержание учебного материала: - Назначение VPN-шлюзов для организации защищенных каналов связи - Криптомаршрутизаторы: интегрированное решение маршрутизации и шифрования

№ п/п	Тематика лекционных занятий / краткое содержание
	- Реализация протоколов IPsec и TLS в аппаратных криптошлюзах - Управление ключами и сертификатами на VPN-устройствах - Отечественные решения: ViPNet, «Континент», «КриптоПро», «МАРШРУТ»
9	Системы обнаружения вторжений (IDS) для защищенных сетей Содержание учебного материала: - Классификация IDS: сетевые (NIDS), хостовые (HIDS), гибридные - Архитектура IDS: сенсоры, консоль управления, база сигнатур - Методы обнаружения: сигнатурный анализ, поведенческий анализ (аномалии), обнаружение Stateful - Размещение сенсоров IDS в сети (на границе, в сегментах, в DMZ) - Отечественные системы IDS: «Аргус», «Рубикон», Positive Technologies (PT Network Attack Discovery)
10	Системы предотвращения вторжений (IPS) и их интеграция в сеть Содержание учебного материала: - Отличие IPS от IDS: активное блокирование атак - Топологии включения IPS (inline vs. passive) - Функции IPS: блокировка пакетов, сброс соединений, изменение правил МЭ - Настройка политик IPS: чувствительность, белые списки, исключения - Проблема ложных срабатываний (false positives) и методы её снижения
11	Анализаторы трафика и системы сетевой разведки (Network Visibility) Содержание учебного материала: - Назначение систем глубокого анализа трафика (DPI, Deep Packet Inspection) - Протоколы мониторинга: NetFlow, sFlow, IPFIX, SNMP - Оборудование для захвата и анализа трафика (сетевые TAP-ы, SPAN-порты) - Системы сетевой разведки для обнаружения аномалий и атак - Примеры: Zabbix, PRTG, DPI-комбайны отечественного производства
12	Криптографические шлюзы и аппаратные модули безопасности (HSM) Содержание учебного материала: - Аппаратные модули безопасности (HSM): назначение, архитектура, сертификация - Функции HSM: генерация и защищенное хранение ключей, аппаратное шифрование, ускорение криптоопераций - Криптографические шлюзы для защиты каналов связи между сегментами сети - Стандарты взаимодействия с HSM: PKCS#11, KMIP, Microsoft CNG - Отечественные HSM: «КриптоПро HSM», «Континент-АП», «Аккорд»
13	Оборудование для изоляции сегментов сети (сетевые диоды, однонаправленные шлюзы) Содержание учебного материала: - Принцип работы сетевого диода (data diode): аппаратная гарантия однонаправленной передачи - Применение в АСУ ТП и сетях с высокими требованиями безопасности - Однонаправленные шлюзы с функцией протокольной трансляции - Примеры: Waterfall, Owl Cyber Defense, отечественные разработки (НТЦ «Протей») - Сравнение с традиционными МЭ и VPN
14	Беспроводное оборудование защищенных сетей (Wi-Fi, Bluetooth, сотовая связь) Содержание учебного материала:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Угрозы для беспроводных сегментов защищенных сетей - Защищенные точки доступа Wi-Fi: поддержка WPA3-Enterprise, 802.1X, RADIUS - Контроллеры беспроводных сетей (WLC) и политики безопасности - Оборудование для обнаружения беспроводных вторжений (WIDS/WIPS) - Оборудование защищенной сотовой связи (LTE/5G с криптографической защитой)
15	Оборудование для создания защищенных каналов с использованием квантового распределения ключей (QKD) Содержание учебного материала: - Принципы квантового распределения ключей (QKD) в телекоммуникационном оборудовании - Устройства QKD: приемники и передатчики на основе фотонов, блоки согласования ключей - Интеграция QKD с классическими VPN-шлюзами (гибридные решения) - Ограничения QKD-оборудования (дальность, скорость, стоимость) - Примеры QKD-оборудования: ID Quantique (Швейцария), QRate (Россия)
16	Системы управления и мониторинга безопасности оборудования (SIEM, SOAR, оркестрация) Содержание учебного материала: - Централизованное управление телекоммуникационным оборудованием в защищенной сети - Протоколы управления: SNMPv3 (шифрование и аутентификация), NETCONF, RESTCONF, SSH - Сбор и анализ логов оборудования в SIEM-системах - Автоматизация реагирования на инциденты через SOAR (Security Orchestration, Automation and Response) - Оркестрация сетевых политик безопасности (закрытие портов, изоляция устройства) - Отечественные решения: MaxPatrol SIEM, Кибербезопасность Positive Technologies, ViPNet Coordinator SIEM

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Исследование процессов преобразования аналогового сигнала в цифровую форму (ИКМ) В результате выполнения работы студент изучит процессы преобразования непрерывного сигнала с ограниченным спектром в сигнал ИКМ (импульсно-кодовая модуляция), включая этапы дискретизации по времени (теорема Котельникова), квантования по уровню (шаг квантования, шум квантования) и кодирования, а также подготовит отчет с анализом зависимости качества восстановленного сигнала от частоты дискретизации и разрядности квантования.
2	Исследование защищенного коммутатора и механизмов сегментации сети (VLAN) В результате выполнения работы студент изучит архитектуру защищенного коммутатора, процессы настройки виртуальных локальных сетей (VLAN) для изоляции трафика, механизмы портовой безопасности (Port Security, ограничение количества MAC-адресов), а также подготовит отчет с выводами о роли VLAN в обеспечении безопасности сегментов сети.
3	Исследование защищенного маршрутизатора и протоколов динамической маршрутизации с аутентификацией

№ п/п	Наименование лабораторных работ / краткое содержание
	В результате выполнения работы студент изучит процессы настройки защищенного маршрутизатора, конфигурации протоколов динамической маршрутизации OSPF/BGP с включенной аутентификацией (MD5, SHA), механизмы фильтрации маршрутов и создания виртуальных маршрутизаторов (VRF), а также подготовит отчет с анализом уязвимостей протоколов маршрутизации и методов их защиты.
4	Исследование межсетевого экрана нового поколения (NGFW) и политик прикладной фильтрации В результате выполнения работы студент изучит процессы настройки межсетевого экрана нового поколения, создания политик безопасности на основе приложений (DPI - глубокий анализ пакетов), механизмы инспектирования SSL/TLS-трафика и блокировки нежелательных сервисов, а также подготовит отчет с рекомендациями по построению политик фильтрации для защищенной сети предприятия.
5	Исследование VPN-шлюза и настройки защищенного канала (IPsec/IKE) В результате выполнения работы студент изучит процессы организации защищенного канала связи с использованием VPN-шлюза, настройки протоколов IPsec в режиме туннеля (ESP, AH), механизмы обмена ключами IKEv1/IKEv2 с аутентификацией по сертификатам и предварительному ключу, а также подготовит отчет с анализом параметров безопасности и производительности VPN-соединения.
6	Исследование системы обнаружения вторжений (IDS) и анализа сигнатур атак В результате выполнения работы студент изучит процессы развертывания сетевой системы обнаружения вторжений (NIDS), настройки сигнатур для выявления известных атак (сканирование портов, SQL-инъекции, попытки переполнения буфера), механизмы сбора и анализа трафика с использованием SPAN-порта или сетевого TAP-а, а также подготовит отчет с выявленными аномалиями и рекомендациями по настройке IDS.
7	Исследование системы предотвращения вторжений (IPS) и режимов активной блокировки В результате выполнения работы студент изучит процессы включения IPS в разрыв канала (inline), настройки политик автоматической блокировки подозрительных пакетов и сброса соединений, механизмы защиты от ложных срабатываний (белые списки, исключения), а также подготовит отчет с оценкой эффективности IPS при различных типах сетевых атак.
8	Исследование аппаратного модуля безопасности (HSM) для генерации и хранения криптографических ключей В результате выполнения работы студент изучит процессы инициализации аппаратного модуля безопасности (HSM), генерации асимметричных ключевых пар внутри защищенной криптографической среды, выполнения операций шифрования и электронной подписи без выгрузки закрытого ключа, а также подготовит отчет с анализом роли HSM в создании доверенной инфраструктуры PKI.
9	Исследование сетевого диода (data diode) для однонаправленной передачи данных В результате выполнения работы студент изучит процессы настройки сетевого диода, обеспечивающего аппаратную гарантию однонаправленной передачи данных, механизмы протокольной трансляции и фильтрации, применение диода для защиты АСУ ТП и сетей с повышенными требованиями к безопасности, а также подготовит отчет с выводами о сценариях использования диода вместо традиционных межсетевых экранов.

№ п/п	Наименование лабораторных работ / краткое содержание
10	Исследование сетевого диода (data diode) для однонаправленной передачи данных В результате выполнения работы студент изучит процессы настройки сетевого диода, обеспечивающего аппаратную гарантию однонаправленной передачи данных, механизмы протокольной трансляции и фильтрации, применение диода для защиты АСУ ТП и сетей с повышенными требованиями к безопасности, а также подготовит отчет с выводами о сценариях использования диода вместо традиционных межсетевых экранов.
11	Исследование оборудования для защиты каналов с квантовым распределением ключей (QKD) В результате выполнения работы студент изучит процессы работы оборудования квантового распределения ключей (QKD), включая генерацию и передачу одиночных фотонов, согласование баз (протокол BB84), оценку квантовой битовой ошибки (QBER) и формирование финального секретного ключа, а также подготовит отчет с выводами о практических ограничениях QKD (дальность, скорость) и его интеграции с классическими VPN-шлюзами.
12	Исследование системы сбора и анализа логов (SIEM) для телекоммуникационного оборудования В результате выполнения работы студент изучит процессы подключения телекоммуникационного оборудования (коммутаторы, маршрутизаторы, МЭ) к SIEM-системе, настройки протоколов сбора логов (Syslog, SNMP, NetFlow), написания правил корреляции для обнаружения аномальной активности, а также подготовит отчет с дашбордом событий безопасности и выявленными инцидентами.
13	Исследование протокола SNMPv3 для защищенного управления сетевым оборудованием В результате выполнения работы студент изучит процессы настройки протокола SNMPv3 на сетевом оборудовании, конфигурации аутентификации (HMAC-MD5/HMAC-SHA) и шифрования (DES/AES) для защиты канала управления, механизмы разграничения доступа по MIB-дереву (View-Based Access Control), а также подготовит отчет с анализом уязвимостей SNMPv1/v2c и преимуществами SNMPv3.
14	Исследование отказоустойчивого оборудования и протоколов резервирования (VRRP, LACP, STP) В результате выполнения работы студент изучит процессы настройки протоколов отказоустойчивости на телекоммуникационном оборудовании: VRRP (резервирование шлюза), LACP (агрегация каналов), RSTP/MSTP (предотвращение петель в сети), механизмы автоматического переключения при отказе узла или канала, а также подготовит отчет с оценкой времени восстановления связи при различных сценариях отказов.
15	Исследование оборудования для глубокого анализа трафика (DPI) и выявления аномалий В результате выполнения работы студент изучит процессы настройки оборудования глубокого анализа пакетов (DPI), механизмы распознавания протоколов прикладного уровня (HTTP, HTTPS, DNS, FTP, BitTorrent), выявления аномалий (аномальный объем трафика, подозрительные имена хостов), а также подготовит отчет с примерами обнаружения скрытых каналов передачи данных и вредоносной активности.
16	Исследование комплексного стенда защищенной сети (маршрутизатор - МЭ - коммутатор - IPS)

№ п/п	Наименование лабораторных работ / краткое содержание
	В результате выполнения работы студент изучит процессы сборки и настройки комплексного стенда защищенной сети, включающего защищенный маршрутизатор, межсетевой экран, коммутатор и систему предотвращения вторжений (IPS), механизмы сквозной фильтрации трафика и изоляции сегментов (DMZ, внутренняя сеть, гостевой сегмент), а также подготовит отчет с проверкой работоспособности всех звеньев защиты и моделированием нескольких типов атак.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным работам
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Голдовский Я.М. Проектирование кампусных сетей : учеб. пособие по дисц. "Сети ЭВМ и телекоммуникации" для студ. спец. "Информатика и вычислительная техника" /; МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2009. - 130 с. : ил. - - Библиогр.: с. 130. - 100 экз. - (в пер.) : 99.86 р.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/10-1289.pdf. (дата обращения 09.06.2026)Текст : непосредственный. 004 Г60
2	ГолдовскийЯ.М. ,Желенков Б.В., Цыганова Н.А. Маршрутизация в компьютерных сетях :	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/DC-407.pdf.(дата обращения 09.06.2026) [Электронный ресурс] 681.3 Г60

	[Электронный ресурс] : учеб. пособие по дисц. "Сети и телекоммуникации" для студ. напр. "Информатика и вычислительная техника" ; МИИТ. Каф. "Вычислительные системы и сети". - М. : РУТ(МИИТ), 2017. - 114 с. - 100 экз. - Б. ц.	
3	В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы : учебное пособие для вузов. - 4-е изд. - СПб. : Питер, 2015. - 944 с. : ил. - ("Учебники для вузов"). - Библиогр.: с. 917. - ISBN 978-5-496-00004-8 (в пер.) : 470.00 р.	научно-техническая библиотека МИИТ(дата обращения 09.06.2026)полочный шифр 004 О-54.
4	Телекоммуникационные и информационные технологии на транспорте России "ТелекомТранс -2008". Шестая Международная научно-практическая конференция (20-22 мая, 2008 г.) : сб. докладов / Ростовский гос. ун-т путей сообщения (РГУПС). - Ростов н/Д : [б.и.], 2008. - 320 с. : ил. - ISBN 978-5-88814-243-1 : Б. ц. - Текст : непосредственный	научно-техническая библиотека МИИТ(дата обращения 09.06.2026)полочный шифр 001-И66

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Современные профессиональные базы данных и информационные справочные системы не требуются.

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

- Microsoft Windows
- Microsoft Office .

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения аудиторных занятий и самостоятельной работы требуются:

- Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET
- Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
- Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

Для проведения лабораторных работ:

- компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.
- В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Зачет в 9 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, к.н. кафедры
«Вычислительные системы и
квантовые коммуникации» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова